REMARKS

This amendment is in response to the Non-Final Office Action dated January 23, 2009 (the "Office Action"). Claims 1-9, 13, and 15-20 are pending in the application. Claims 10-12 were previously cancelled without prejudice or disclaimer. Claims 1, 7, and 13 have been amended. No new matter has been added. Support for the claim amendments can be found at least at paragraph [0035] of the application.

Claims 1-6 are Allowable

The Office has rejected claims 1-6, under 35 U.S.C. § 103(a), as being unpatentable over U.S. Published Application No. 2002/0176579 ("Deshpande") in view of U.S. Published Application No. 2003/0163733 ("Barriga-Caceres"). Applicants respectfully traverse the rejections.

The cited portions of the above-cited references do not disclose or suggest the specific combination of claim 1. For example, the cited portions of the above-cited references fail to disclose or suggest a network access hub operable to receive an initial set of credentials from a user via a computing device, where the initial set of credentials includes biometric user information, as in claim 1.

In contrast to claim 1, Deshpande describes a user/device required to provide identification information such as a user name to determine whether and what types of services may be provided and authentication information such as a password to confirm proper usage of the services. *See* Deshpande, [0025]. Deshpande further discloses that if the user/device is authenticated, there may be modes on the device or on a hotspot service provider to provide appropriate security, e.g., a unique user/device identification or a unique IP address. *See* Deshpande, [0026]. The cited portions of Deshpande do not disclose or suggest biometric user information. Instead, Deshpande discloses automatically getting device-based information related to a mobile device. Therefore, the cited portions of Deshpande fail to disclose or suggest a network access hub operable to receive an initial set of credentials from a user via a computing device, where the initial set of credentials includes biometric user information, as in claim 1.

In further contrast to claim 1, Barriga-Caceres describes credentials such as digital certificates, short-time certificates, or temporary tickets or tokens that may be used by a user in

authentication or authorization procedures. *See* Barriga-Caceres, [0007]. The cited portions of Barriga-Caceres do not disclose or suggest biometric user information. Therefore, the cited portions of Barriga-Caceres fail to disclose or suggest a network access hub operable to receive an initial set of credentials from a user via a computing device, where the initial set of credentials includes biometric user information, as in claim 1.

Therefore, the cited portions of the above-cited references, individually or in combination, fail to disclose or suggest at least one element of claim 1. Hence, claim 1 is allowable. Claims 2-6 are allowable, at least by virtue of their dependence from claim 1.

Claims 7-9 are Allowable

The Office has rejected claims 7-9, under 35 U.S.C. § 103(a), as being unpatentable over Deshpande in view of Barriga-Caceres. Applicants respectfully traverse the rejections.

The cited portions of the above-cited references do not disclose or suggest the specific combination of claim 7. For example, the cited portions of the above-cited references fail to disclose or suggest receiving a first set of credentials including biometric user information, as in claim 7.

In contrast to claim 7, Deshpande describes a user/device required to provide identification information such as a user name to determine whether and what types of services may be provided and authentication information such as a password to confirm proper usage of the services. *See* Deshpande, [0025]. Deshpande further discloses that if the user/device is authenticated, there may be modes on the device or on a hotspot service provider to provide appropriate security, e.g., a unique user/device identification or a unique IP address. *See* Deshpande, [0026]. The cited portions of Deshpande do not disclose or suggest that credentials include biometric user information. Instead, Deshpande discloses automatically getting device-based information related to a mobile device. Therefore, the cited portions of Deshpande fail to disclose or suggest receiving a first set of credentials including biometric user information, as in claim 7.

In further contrast to claim 7, Barriga-Caceres describes credentials such as digital certificates, short-time certificates, or temporary tickets or tokens that may be used by a user in authentication or authorization procedures. *See* Barriga-Caceres, [0007]. The cited portions of Barriga-Caceres do not disclose or suggest biometric user information. Therefore, the cited

portions of Barriga-Caceres fail to disclose or suggest receiving a first set of credentials including biometric user information, as in claim 7.

Therefore, the cited portions of the above-cited references, individually or in combination, fail to disclose or suggest at least one element of claim 7. Hence, claim 7 is allowable. Claims 8-9 are allowable, at least by virtue of their dependence from claim 7.

Claims 13 and 15-20 are Allowable

The Office has rejected claims 13-20, under 35 U.S.C. § 103(a), as unpatentable over Deshpande in view of Barriga-Caceres. Claim 14 has been cancelled without prejudice of disclaimer. Applicants respectfully traverse the remaining rejections.

The cited portions of the above-cited references do not disclose or suggest the specific combination of claim 13. For example, the cited portions of the above-cited references fail to disclose or suggest an authorization engine operable to issue a token to an electronic device communicatively coupled to at least a first hotspot of a plurality of hotspots in response to receiving biometric user information, as in claim 13.

In contrast to claim 13, Deshpande describes a user/device required to provide identification information such as a user name to determine whether and what types of services may be provided and authentication information such as a password to confirm proper usage of the services. *See* Deshpande, [0025]. Deshpande further discloses that if the user/device is authenticated, there may be modes on the device or on a hotspot service provider to provide appropriate security, e.g., a unique user/device identification or a unique IP address. *See* Deshpande, [0026]. The cited portions of Deshpande do not disclose or suggest authorization in response to biometric user information. Instead, Deshpande discloses authorization based on automatically getting device-based information related to a mobile device. Therefore, the cited portions of Deshpande fail to disclose or suggest an authorization engine operable to issue a token to an electronic device communicatively coupled to at least a first hotspot of the plurality of hotspots in response to receiving biometric user information, as in claim 13.

In further contrast to claim 13, Barriga-Caceres describes credentials such as digital certificates, short-time certificates, or temporary tickets or tokens that may be used by a user in authentication or authorization procedures. *See* Barriga-Caceres, [0007]. The cited portions of Barriga-Caceres do not disclose or suggest biometric user information. Therefore, the cited

portions of Barriga-Caceres fail to disclose or suggest an authorization engine operable to issue a token to an electronic device communicatively coupled to at least a first hotspot of the plurality of hotspots in response to receiving biometric user information, as in claim 13.

Therefore, the cited portions of the above-cited references, individually or in combination, fail to disclose or suggest at least one element of claim 13. Hence, claim 13 is allowable. Claims 15-20 are allowable, at least by virtue of their dependence from claim 13. Further, the dependent claims recite additional elements not disclosed or suggested by the cited portions of the above-cited references.

For example, the cited portions of the above-cited references fail to disclose or suggest a data service comprising a unified messaging mailbox, as in claim 18. In contrast to claim 18, Deshpande describes synchronizing a wireless device to e-mail associated with user/device identification information. *See* Deshpande, [0017]. Deshpande also discloses providing location-based services to a wireless device. *See* Deshpande, [0041]. The cited portions of Deshpande do not disclose or suggest a unified messaging mailbox. In further contrast to claim 18, Barriga-Caceres describes single sign-on functionality for multiple mobile network operators. *See* Barriga-Caceres, [0011]. The cited portions of Barriga-Caceres do not disclose or suggest a unified messaging mailbox. Hence, claim 18 is allowable for at least this additional reason.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the references as applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims.

Any changes to the claims in this response, which have not been specifically noted to overcome a rejection based upon the cited art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

4-20-2009
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicants
Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)